Supplementary Submission No. 7.1

AUSTRALIAN BANKERS' ASSOCIATION INC.

Tony Burke
Director

Level 3, 56 Pitt Street
Sydney NSW 2000
Telephone: (02) 8298 0409
Facsimile: (02) 8298 0402

14 October 2009

Mr Jerome Brown
Secretary
House Standing Committee on Communications
PO Box 6022
House of Representatives
Parliament House
CANBERRA ACT 2600

Dear Mr Brown,

Cybercrime Inquiry

Thank you for the opportunity to appear before the Committee on 8 October 2009.

The Committee asked us to respond with further detail on a number of points:

(1) The Australian Bankers' Association's ("**ABA**") targeted campaign on "money mules";

(2) Industry views on bank "white listing";

(3) Telephone banking risks and mitigation strategies; and

(4) The need for amendments to the *Spam Act 2003* ("*Spam Act*") to cover the use of spam in delivering malicious code ("malware").

Further information on each of these points follows.

Money mules

In 2008 the ABA did a joint media release and media campaign with the Australian Federal Police warning against becoming a "money mule"[1]. Money mules are the middlemen for criminals who have obtained funds by online fraud

[1] Money mules explained: Media Release available on-line at the ABA's website at: http://www.bankers.asn.au/DONT-BE-A-MULE---SAY-NO-TO-TRANSFERRING-MONEY-FOR-CRIMINALS/default.aspx.

Fact sheet also available at: http://www.bankers.asn.au/default.aspx?ArticleID=1219

though phishing or hacking. The criminals need a "mule" to launder the funds obtained as a result of illegal activities.

After being recruited by the criminals, money mules receive funds into their bank accounts and then withdraw the money and send it to a designated account (domestic or offshore), using a wire transfer service and retain a 'commission' payment.

This year, the ABA decided to target a specific section of the community, university students, at a time when they may be seeking holiday employment. We did this based on feedback received from various stakeholders, including law enforcement, that students may be vulnerable to this type of offer.

The ABA has contacted thirty eight (38) universities throughout Australia to ask them if they can assist in disseminating the information to their students. The response has been very positive and enthusiastic. Universities have advised the ABA that they will provide the information via hard copy, their internet and intranet sites and also through direct email and noticeboards for their students.

The campaign was launched on 12 October 2009.

Attached for your information are the:

- Joint media release ABA/ AFP warning students of mule scams; and
- Fact sheet on mule scams (tailored for students)

White listing

The general strategy to date in relation to cybercrime could be described very simply as "black listing". For example, banks build very strong barriers against attacks, identify the likely sources of those attacks, then black list the related IP addresses both privately (within their networks) and with public mail servers.

"White listing" takes a different approach: anything that is deemed to be safe is white listed and nothing else is given permission to enter the environment controlled by the white listing service.

There are a number of "white listing" methods that can be used by service providers, infrastructure providers and consumers to help protect against cybercrime. These can be broken down into three main methods, depending on where the white list is managed and enforced.

A white list of "known good" locations of banks could prove useful to vendors of security software, who could use such information to detect if a site purporting to be a banking website is legitimate or fraudulent. Similarly, internet service providers could potentially use similar techniques to help protect their customers from fraudulent or malicious sites by comparison with a "white list".

However, the majority of security solutions already provide a similar level of protection, as the "known good" domain names and IP addresses for banks are already in the public domain.

Service providers such as banks can "white list" customers as having come from a known good location (for example, from the IP address associated with their home or work Internet connection) and currently employ similar techniques for fraud detection.

While "white listing" of this nature would address some threats, we believe that it would also restrict the ability of customers to access banking services while away from their "registered" location, without any significant benefit of corresponding protection. There are also technical limitations on the effectiveness of such techniques, due to a large number of customers having dynamically allocated IP addresses.

Case studies the ABA has seen on "white listing" have been based on much smaller organisations than our larger banks, with much less complex operating environments.

"White listing" would require very careful design and implementation to avoid the risk of legitimate traffic being blocked in what are very sophisticated, high-transaction, high-availability environments. Our members would not wish to see a situation in which diminution of services occurred as a result of the use of "white listing" or a content blocking service.

The adoption of "white listing" could also create additional complexity and risk for the extensive inter-bank arrangements and networks in place in Australia and internationally.

"White listing" solutions are one possible measure that may assist in addressing some facets of the cybercrime threat, but the ABA and its member banks believe that the best approach is a combination of measures, which respond to and evolve with the current threat profile, and not a single solution.

We remain willing to explore any techniques which may support the protection of our customers against cyber threats, which the Government may have in mind now, or may wish to consider in the future.

Telephone Scams

The ABA has seen reports of incidents in which criminals are attempting to obtain consumers' personal information via telephone. In one example we have seen, the criminals claim that they are from a company which has chosen the consumer to be provided with a credit card with a pre-approved line of credit.

The consumer is told the credit card will be sent to them via mail if they provide the following information to the company: their name, residential address, driver's licence, date of birth and annual income.

The key message that the ABA and its members have been providing over many years now is "Do not give out your personal or account information over the phone unless you have initiated the contact with the institution concerned."

Although telephone banking users will be asked for a password during a banking session, our members never ask the customer to provide their Personal

Identification Number (PIN). Banks tell their customers that their PIN must be kept safe at all times, and must never be divulged to any person or system, including a telephone banking system.

Other relevant customer safety messages in this area to date have included:

- *Be very wary of unsolicited calls or e-mails requesting personal information or card numbers. You should never divulge your PIN.*
- *Always do your homework before you agree to any offer you receive over the telephone and never agree to any offer that you are not completely sure about; and*
- *If the offer sounds too good to be true, then it probably is.*

***Spam Act* 2003 (Cth)**

Sending "unsolicited electronic messages" ("spam") is not a criminal offence in Australia at present under the *Spam Act*, although civil penalties do exist under that Act for the dissemination of spam. The ABA understands that criminals have been using spam to deliver malware to consumers.

It may be desirable for a single offence provision to be created for the sending of malware by spam. Banks would welcome consultation on this matter, following an initial analysis by the Commonwealth of existing provisions that may cover the field. The creation of a single offence may have the benefit of simplifying prosecutions in this area.

Consultation would need to include consideration of a range of issues, including but not limited to, the means by which legitimate activities by our members and others were not impacted, and liabilities were not extended. We look forward to further engagement on this matter with the Government.

Please let me know if we can assist the Committee with any further information. We look forward to the Committee's report.

Yours sincerely

_____

Tony Burke

AUSTRALIAN BANKERS' ASSOCIATION INC.

AUSTRALIAN FEDERAL POLICE

Joint media release

Students – don't fall for a mule scam when seeking holiday jobs

Sydney, 12 October, 2009: Banks and the Australian Federal Police (AFP) have targeted university students to warn them about money mule scams when seeking holiday employment.

The Australian Bankers' Association (ABA) and the AFP have prepared a fact sheet, 'Warning to students – don't get caught by mule scams'. It warns students of the scams which trap them into laundering money for criminals by becoming a money mule.

A money mule is someone who allows their bank account to be used to receive stolen funds which are transferred to a designated account (domestic or offshore) using a money-remitting or wire service, minus a commission payment.

The mule is usually approached online via email, instant message or criminals may advertise on legitimate employment websites and publications.

AFP Acting National Manager High Tech Crime Operations, Karl Kent, said students are vulnerable at this time of the year as they are seeking employment during the holiday period.

Commander Kent said: "You would be very suspicious if someone you didn't know asked you to carry a package or money overseas. Similarly, you should be very suspicious about someone asking you to transfer money in and out of your bank account to other accounts."

"These scams involve you in a criminal enterprise and there are serious penalties under Australian and international laws for laundering money."

"The prospect of making easy money may appear attractive. However, any 'commission' payments will be recovered as they are the proceeds of crime and the person - the money mule - could become the subject of a police investigation that could lead to a maximum penalty of 20 years' imprisonment."

"If you are in Australia on a student visa, having a criminal conviction recorded against you may mean that you are not able to complete your studies at an Australian institution."

Usually, criminals send out millions of fraudulent job offer emails to random email addresses in the hope of involving unsuspecting, innocent persons in their criminal activity. You should ignore such emails and immediately delete them.

Sometimes the criminals even use legitimate employment websites to post their scam job ads. Once you respond to the advertisement, the criminal will ask that money be moved through your bank account. Don't be fooled: when you transfer money in this way the law views you as being a criminal too.

David Bell, Chief Executive of the ABA, said: "Customers who participate risk prosecution, will have their commission confiscated as proceeds of crime, their banking facilities will be withdrawn and they could have their identity stolen by the criminals as well."

"The criminals who have recruited a mule don't need him or her once the money has been cycled through accounts. When they are finished with you, they leave you to face the police and the courts alone."

"If international students become involved and banking facilities are withdrawn, this can have major ramifications as many students rely upon their bank account to obtain the financial support that they need from their families, friends and organisations back home to complete their studies."

Banks and police advise that if you are offered an opportunity of making easy money and the offer seems too good to be true, then it probably is!

Following the tips below can help you prevent becoming entangled a money mule scam:

- Be cautious about accepting any unsolicited offers or opportunities that offer you the chance of making money simply by moving money in and out of any bank account.
- Be wary of any offers from people or companies overseas as it makes it harder to check if they or their offers are legitimate.
- Do not rely on weblinks in any e-mail or document that provide you with a reference to the company's or person's website or e-mail address as being proof that the company or person is legitimate.
- Take steps to verify the background of any company or person which makes you a job offer. For example, initiate your own separate check to verify that they have a known registered address. For any company that carries on business in Australia, you can also check with the Australian Securities and Investments Commission (ASIC) if the company is a registered business or company by using the free search available at ASIC's home page: www.asic.gov.au.
- Never provide your confidential banking details to anyone – this includes your PIN and Internet banking login or passwords.
- Always guard your personal information and be very suspicious if someone asks you for your personal details, including your banking details. Be very careful about providing any details that identify you, such as your date of birth, gender, nationality, Higher Education Contribution Scheme (HECS) number, Tax File Number (TFN), passport number, driver's licence number or any bank account details.
- Be wary of people asking you for financial assistance – never send money to any person or organisation you do not know or have an involvement with, particularly by money or wire transfer, as these funds cannot be recovered by banks.
- Be cautious of someone asking for details of your financial status, such as how much you earn, how much you have saved or what accounts you hold.

Background notes for editors

A fact sheet for students with an example of a scam email, a diagram of how the money mule recruitment process works and a case study of a conviction is available on the following websites: www.bankers.asn.au/studentmule or www.afp.gov.au.

For further information or to arrange an interview:

Heather Wellard, ABA PR
Phone: 02 8298 0411 Mobile: 0409 830 439

AFP National Media
Phone: 02 6275 7100

ENDS

Warning to students – don't get caught by mule scams

Job offers that involve transferring money or goods for someone you don't know are nearly always a scam. Criminals are trying to use you as a money mule to transfer and disguise their proceeds of crime.

Participating in these scams and transferring this money could lead to a police investigation and criminal charges against you for your part in a criminal enterprise. This activity is also unacceptable to banks and may result in the withdrawal of your banking facilities.

This fact sheet, compiled by the Australian Bankers' Association (ABA) and the Australian Federal Police (AFP), will help you recognise these types of scams and avoid becoming involved in unlawful activity.

WHAT IS A MONEY MULE?

Money mules are the 'middlemen' for criminals who have stolen funds. The criminals need a mule to help cover their tracks and transfer the stolen funds around or out of the country on their behalf.

Typically, a money mule will be requested to receive funds into his or her own bank account and then to send those funds to someone else's account (as nominated by the criminal to the mule). The funds might be transferred using bank accounts (either in person at a branch, or via an ATM or the Internet) or through a money or wire transfer service.

Mules are usually offered a 'commission' by the criminal for their part in the criminal enterprise, which is normally a small percentage of the stolen funds, as payment for their services. A 'commission' for the mule's role in the crime need not be provided in cash or via funds placed into your bank account. In variations of these scams, the mule may receive their 'commission' by being provided with goods in return for the service they are providing, rather than a cash commission. For example, if you act as a mule, the criminal may offer you goods as your 'payment' for your part in the mule scam. The goods might include things like laptop

computers, Personal Digital Assistants (PDAs) or mobile phones. These goods themselves have usually been purchased by the criminal with stolen funds. Make no mistake: receiving these goods is receiving a 'commission' for playing your part in a crime. If you receive a benefit of any kind, you may be found to have received a benefit relevant to your role in the crime.

MONEY MULE SCAMS – HOW THEY WORK

Australian law enforcement and the banks have generally seen that criminals recruit unsuspecting innocent people in their illegal activities through:

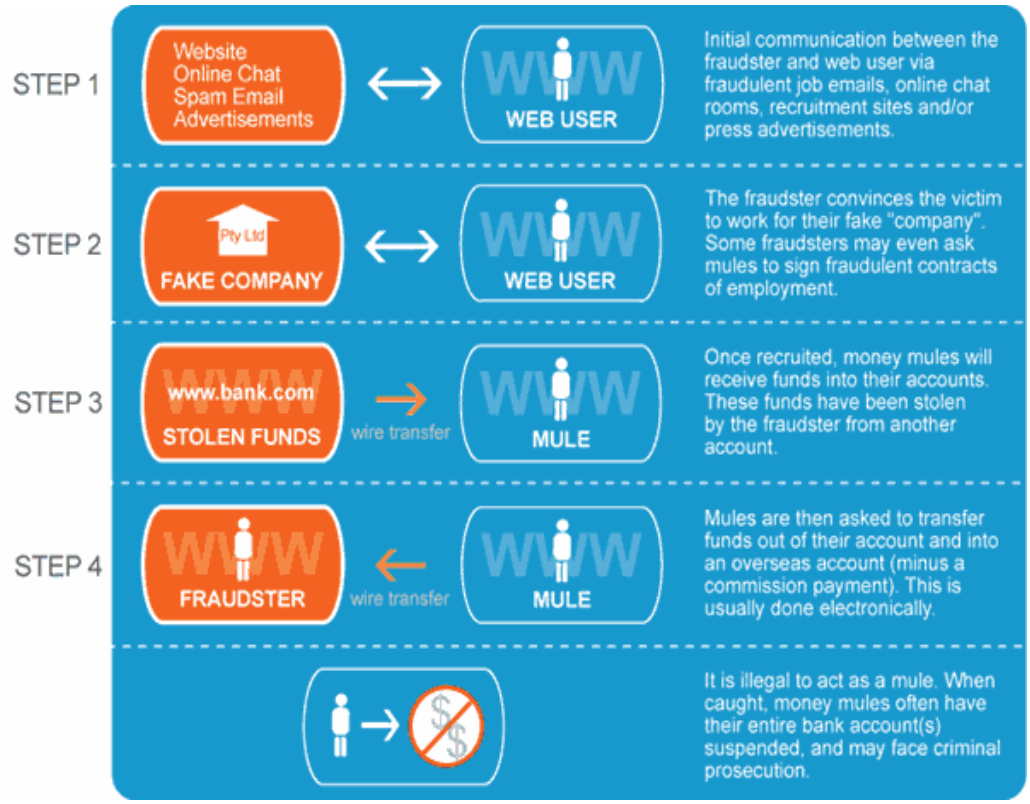
1) **Job scams** - fraudulent employment advertisements are posted online or e-mails are sent to random addresses promising quick commissions in return for receiving money or goods and transferring it elsewhere. These are not legitimate jobs!!

2) **Romance scams** – singles are asked to receive money and send it elsewhere duped by the promise of a relationship.

Criminals may also use online chat rooms, social networking sites, hoax websites, fake advertisements and fake profiles to recruit mules and to try to persuade people to take part in criminal activity. There have also been cases of people being approached directly to become a mule where they have published their resumes online.

The AFP and the ABA advise that you should ignore these approaches and immediately delete suspicious e-mails and/or ignore online contact. (Fact sheet continues over the page)

The following diagram illustrates how a mule scam is perpetrated:



(Source: Australian Federal Police)

EXAMPLE OF A JOB SCAM RECRUITING MULES VIA E-MAIL

Money mule advertisements or offers can take a variety of forms and the criminals may additionally use a fake website to add authenticity to the scam. Some of the adverts can direct you to websites which can infect your computer with viruses.

The criminals can also use spam e-mail to reach millions of addresses in the hope they will convince a person to respond to the offer. The criminals prey on people who need to make extra cash quickly and easily by offering jobs that only require you to have Internet access and to only work a few hours a week.

Not only do the criminals use you and your bank account to transfer their stolen funds, but they may also steal your money from your bank account as well.

If you are looking at any job offer that sounds a bit like this, you should ask yourself the following questions:

- Why is no interview conducted for the job offer?
- Why would someone whom you have never met entrust you with their money?
- Why do they need your banking details?
- Why do they need to transfer money via Australia when their 'employer' (the criminal) is located in another country?

These circumstances are highly unusual and should raise your suspicion.

Below are two examples of scam e-mails that attempt to recruit a mule through a job offer.

The first e-mail is an example of the victim being asked to move money through bank accounts for a 'commission':

From: alexis luong

Sent: Tuesday, 5 February 2008 11:37 PM

To: [redacted]

Subject: start your career with us

Welcome to the Service!

We are very glad that you wish to join our team, will be delighted to have you work with us. The position of Assistant provides support filling the transactions of our customers.

We deal exclusively with private clients- that have special requirements for high speed of receiving funds for their business.

This way we can offer a new kind of financial and banking service to our clients - and we would like you to work as an Assistant (part-time job 3-4 hours a day except holidays).

At first your work would be very basic, yet meticulous -you will make transfers for our clients to suit their needs. Our managers will assist you during the trial period and explain everything you will need to know.

We offer an extremely competitive graduated salary: for the first month you will receive up to $2000 for your work the next month your salary will be increased if you do your work accurately and on time.

Now you are only one step away from successful career.

All you need is to send an e-mail to:

With phone numbers and times to reach you, and one of our representatives will contact you and answer all your questions.

Thank you in advance,

The second e-mail example we have provided below is more sophisticated.

Here, the victim is asked to become a 'data entry' clerk for the company. When you accept the job offer you may be asked to provide the company with an 'administration fee' before they send you further details of the job. You dutifully send your money off (which you will never see again!) and the company then asks you to receive or transfer funds. In other words, you are asked to become a money mule for them, just not in so many words!

You will notice that the e-mail contains weblinks which have been removed. Many of the mule scams being used have weblinks that contain malware (malicious software) which automatically downloads itself onto your computer.

Most of this malware is designed to enable the criminal to infiltrate your computer so that they can steal confidential information about you. That might include passwords, your Internet banking logins or even sensitive personal information like your date of birth and Tax File Number (TFN). You may not even know that the malware has been installed on your computer. The criminals figure that if they can't use you as a mule, they might as well try to steal your identity for their own future use in their criminal acts.

That's why it's important to delete any e-mails from sources you don't recognise – don't even open them and never click on a link in an e-mail from someone you don't know or recognise.

To: [redacted]

Subject: LEGITIMATE WORK from home data entry job

The following news release from [redacted] *Corporation has been forwarded to you by Cathy at*

If you wish to stop receiving these news releases, please contact the sender. Comments from the sender:

Dear Friend,

My name is [redacted] *If you're interested in Making Money and Improving Your Life, then please pay careful attention to this letter.*

Would you like to earn an EXTRA $200 EVERYDAY? for just 15 minutes work? You could quit your job and make double the money at home working for yourself.

Companies are currently looking for data entry workers worldwide to enter data online. Rates of pay are excellent from $200 a day and up. We have over 100,000 current members earning extra money from their own home.
You don't need any prior experience to work entering data; access to the internet is all that is needed. You can simply follow our step by step guide and work whenever you want for how long you

want. You will be in control of your own working hours, the more you work the more you earn. We have many students, work from home moms and retired men and women who are making extra cash, We lead you by hand to earning a substantial income online!

Here and Have a look:

Anyone can do it – It really is easy, you can simply signup for data entry accounts which we tell you then submit the forms with the data we provide and lastly watch your account as money adds up daily. These companies need people like you to enter data as it spreads word about their products helping them to generate sales. This is how they can pay you so much; they are splitting their profits with you. You will be paid via check, wire transfer or.

This work is fully legal; You may enter data for over 70,000 different companies. We provide an online catalog of companies, organized into relevant categories (health, money, employment etc). Simply look for companies you would like to join according to how much they pay. You will never submit any forms with data that is objectionable.

Again it takes just minutes to signup with each company, and it is 100% FREE. Our Top member is earning $600 – $1000 every day, why couldn't you?

Our most dedicated members are earning $200+ every day the more forms you submit usually the more money you will make. The amount each company pays varies from $20 – $100 per form. This money will mount in your account every day!

Be a member by clicking join us button at this link:

This is a one time adv. e-mail only and you won't received further mailings about this. If you would like to opt-out just send an e-mail with "Opt Out in the subject line to the address given below.

Sincerely,

[redacted]

Thank you.

ROMANCE SCAMS

Internet dating websites and chat rooms have increased in popularity over recent years with many singles finding it an ideal and convenient way to meet people.

Unfortunately banks are aware of criminals who find their victims by posing as singles, publishing fake profiles and prowling online chat rooms seeking to defraud singles. In the cases seen by banks and police, the criminals cultivate their victims over weeks and months to gain their trust before reeling them in with requests for money or assistance. The request for money might be to help a sick relative or to pay for airfares to enable a meeting.

In one scam, the single female located overseas tells the single male that her friend is sending money so the male can onforward that money overseas to pay for airline tickets. The reason given is that there are problems getting money out of the country. The funds that are received are the proceeds of crime.

In another scam, the single female is approached by a single male who declares undying love very soon after contact and then seeks a money transfer for a sick relative. Both of these scams prey on the good nature of the victim but are trying to involve the victim in criminal activity.

Finally, be aware that scammers might be asking for personal information in order to commit identity theft. It is important to guard this personal information and be wary if you are being asked for too many details about your financial status.

BREAKING THE LAW

The funds that the criminals need transferred are usually the proceeds of crime. Banks and police advise that, in some cases, the criminals who have used you as a mule may have links to organised crime. They are not people you want to become associated with.

Participating in these scams and transferring money could lead to a police investigation and criminal charges against you. Although the offer and commission may seem attractive, any commission payments will be recovered from you anyway as the proceeds of crime.

Acting as a money mule can also result in a criminal conviction for an offence that could lead to the imposition of a maximum penalty of 20 years' imprisonment.

Such actions by you are also unacceptable to banks and will usually result in the withdrawal of your banking facilities.

If you are in Australia on a student visa, being prosecuted for a criminal offence or having a criminal conviction recorded against you, may mean that you are not able to complete your studies at an Australian institution.

If you are an international student and your banking facilities are withdrawn, this can have major ramifications as many students rely upon their bank account to obtain the financial support that they need from their families, friends and organisations back home to complete their studies.

SO HOW CAN I AVOID BECOMING INVOLVED IN A MONEY MULE SCAM?

If you are offered an opportunity of making easy money and the offer seems too good to be true, then it probably is!

Following the tips below can help you prevent becoming entangled a money mule:

- Be cautious about accepting any unsolicited offers or opportunities that offer you the chance of making money simply by moving money in and out of any bank account.
- Be wary of any offers from people or companies overseas as it makes it harder to check if they or their offers are legitimate.
- Do not rely on weblinks in any e-mail or document that provide you with a reference to the company's or person's website or e-mail address as being proof that the company or person is legitimate.
- Take steps to verify the background of any company or person which makes you a job offer. For example, initiate your own separate check to verify that they have a known registered address. For any company that carries on business in Australia, you can also check with the Australian Securities and Investments Commission (ASIC) if the company is a registered business or company by using the free search available at ASIC's home page: www.asic.gov.au.
- Never provide your confidential banking details to anyone – this includes your PIN and Internet banking login or passwords.
- Always guard your personal information and be very suspicious if someone asks you for your personal details, including your banking details. Be very careful about providing any details that identify you, such as your date of birth, gender, nationality, Higher Education Contribution Scheme (HECS) number, Tax File Number (TFN), passport number, driver's licence number or any bank account details.
- Be wary of people asking you for financial assistance – never send money to any person or organisation you do not know or have an involvement with, particularly by money or wire transfer, as these funds cannot be recovered by banks.
- Be cautious of someone asking for details of your financial status, such as how much you earn, how much you have saved or what accounts you hold.

WHAT IF I HAVE REPLIED TO A MULE SCAM OFFER?

If you have received money in your bank account, transferred or attempted to transfer money overseas, or disclosed any of your bank account details and you think you have been involved in money mule scam, please immediately contact your bank or other financial institution. You could be at risk of having your identity stolen by the criminals and your bank account drained of funds.

MORE INFORMATION

Other websites that may be of interest:

www.protectfinancialid.org.au

www.bankers.asn.au

www.afp.gov.au

Created: October 2009

Internet: www.bankers.asn.au www.afp.gov.au

Phone: 02 8298 0417 Fax: 02 8298 0402